TEMA 3

Anillos de polinomios.

Ejercicio 1. Calcula $(2x^3 + 3x^2 + 1)(x^2 + 2x + 3)$ en $\mathbb{Z}_6[x]$.

Ejercicio 2. Calcula el cociente y el resto de dividir $2x^4 + 3x^3 + x^2 + 6x + 1$ entre $3x^2 + 1$ en $\mathbb{Z}_7[x]$ y en $\mathbb{Z}_{10}[x]$.

Ejercicio 3. Comprueba que $x^4 + 1$ es reducible en $\mathbb{Z}_p[x]$ para $p = 2, 3, 5, 7, 11, 13, 17$.

En general se tiene que $x^4 + 1$ es reducible en $\mathbb{Z}_p[x]$ para cualquier número primo.

- Si a es tal que $a^2 \equiv -1 \pmod{p}$ entonces $(x^2 + a)(x^2 - a)$ es una factorización de $x^4 + 1$ en $\mathbb{Z}_p[x]$.
- Si a es tal que $a^2 \equiv 2 \pmod{p}$ entonces $(x^2 + ax + 1)(x^2 - ax + 1)$ es una factorización de $x^4 + 1$ en $\mathbb{Z}_p[x]$.
- Si a es tal que $a^2 \equiv -2 \pmod{p}$ entonces $(x^2 + ax - 1)(x^2 - ax - 1)$ es una factorización de $x^4 + 1$ en $\mathbb{Z}_p[x]$.

Y se tiene que para cualquier primo p, hay en $\mathbb{Z}_p$ una raíz cuadrada de -1, de 2 o de -2.

Ejercicio 4. Sean $p(x) = x^4 + 2x^2 + 2x + 1$, y $q(x) = x^3 + 2x^2 + x + 2$ dos polinomios con coeficientes en $\mathbb{Z}_3$. Sean $r(x) = p(x) \text{ mód } q(x)$ y $s(x) = q(x) \text{ mód } r(x)$.

- Calcula todos los divisores de $p(x)$ (hay 8 en total, cuatro de ellos mónicos), de $q(x)$ (también hay 8) de $r(x)$ (en total 6) y $s(x)$ (hay 4).
- Calcula todos los divisores comunes de $p(x)$ y $q(x)$; de $q(x)$ y $r(x)$; y de $r(x)$ y $s(x)$.
- Calcula el mínimo común múltiplo de $p(x)$ y $q(x)$.

Ejercicio 5. Calcula un máximo común divisor de $a(x)$ y $b(x)$ en los siguientes casos:

1. $a(x) = x^4 + 2x^2 + 1, b(x) = x^4 - 1$ en $\mathbb{Q}[x]$.
2. $a(x) = x^4 + 2x^2 + 1, b(x) = x^2 + 2$ en $\mathbb{Z}_3[x]$.

Ejercicio 6. Calcula, si es posible, $u(x), v(x) \in \mathbb{Z}_7[x]$ tales que

$$(x^2 + 3x + 3) \cdot u(x) + (x^3 + 2x + 4) \cdot v(x) = x + 2$$

Ejercicio 7. Demuestra que la ecuación

$$(x^4 + 2x^2 + 1)\mathcal{X} + (x^4 - 1)\mathcal{Y} = 3x^3 + 3x$$

tiene solución en $\mathbb{Q}[x]$, y halla una solución.

Ejercicio 8. Calcula las raíces en $\mathbb{Z}_5$ del polinomio $x^2 + x + 4$.

Ejercicio 9. Calcula las raíces en $\mathbb{Z}$ del polinomio $x^4 - x^3 + x^2 - x - 10$.

Ejercicio 10. Calcula en $\mathbb{Q}[x]$ el resto de dividir

1. $x^7 + x^2 + 1$ entre $x - 1$,

2. $x^n + 1$ entre $x - 1$.

Ejercicio 11. Calcula en $\mathbb{Z}_5[x]$ el resto de dividir $x^n + 2$ entre $x + 4$.

Ejercicio 12. Demuestra que el polinomio $x^n + 1$ no tiene raíces múltiples en $\mathbb{R}$.

Ejercicio 13. Determina cuáles de los siguientes polinomios tienen raíces múltiples en $\mathbb{C}$.

1. $x^3 - 3x^2 + 3x - 1$,

2. $x^3 + x^2 + 1$,

3. $x^4 + x^3 + x^2 + x + 1$.

Ejercicio 14. Encuentra todas las raíces de $x^2 - 1 \in \mathbb{Z}_8[x]$. Da dos factorizaciones distintas de $x^2 - 1$ como producto de polinomios mónicos.

Ejercicio 15. Calcula un polinomio $p(x) \in \mathbb{Q}[x]$ tal que $p(2) = 0, p(1) = -2, p(3) = 1$ y $p(-1) = 2$.

Ejercicio 16. Calcula un polinomio $p(x) \in \mathbb{Z}_5[x]$ tal que $p(2) = 1, p(3) = 2$ y $p(4) = 1$.

Ejercicio 17. Calcula un polinomio $p(x) \in \mathbb{Z}_7[x]$ tal que $p(2) = 3$, $p'(2) = 5$, $p(4) = 1$.

Ejercicio 18. Comprueba que los polinomios $x^3 + x^2 + x + 1$ y $x^2 + 2x + 1$ determinan la misma aplicación $f : \mathbb{Z}_3 \to \mathbb{Z}_3$.

Ejercicio 19. Calcula un polinomio mónico, con coeficientes en $\mathbb{Z}_5$, de grado 5, que tenga a 1 como raíz doble, y que al dividirlo por $x^2 + 2x + 3$ de resto $3x + 1$.

Ejercicio 20 (Método de interpolación de Lagrange)**.** Sea K un cuerpo, y $a_0, a_1, \cdots, a_m$ elementos distintos de K. Consideramos los polinomios:

$$p_0(x) = \frac{(x-a_1)(x-a_2)\cdots(x-a_m)}{(a_0-a_1)(a_0-a_2)\cdots(a_0-a_n)} = \prod_{k=1}^{m} \frac{(x-a_k)}{(a_0-a_k)}$$

$$p_1(x) = \frac{(x-a_0)(x-a_2)\cdots(x-a_m)}{(a_1-a_0)(a_1-a_2)\cdots(a_1-a_n)} = \prod_{k\neq 1}^{m} \frac{(x-a_k)}{(a_1-a_k)}$$

$$p_m(x) = \frac{(x-a_0)(x-a_1)\cdots(x-a_{m-1})}{(a_m-a_0)(a_m-a_1)\cdots(a_m-a_{m-1})} = \prod_{k=0}^{m-1} \frac{(x-a_k)}{(a_m-a_k)}$$

es decir, $p_i(x)$ es el producto de todos los polinomios de la forma $(x-a_j)$, donde j toma todos los valores (salvo i) desde 0 hasta m, dividido todo por el resultado de evaluar ese producto en a_i.

- Comprueba que

$$p_i(a_j) = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j \end{cases}$$

Sean ahora $b_0, b_1, \cdots b_m \in K$, y $p(x) = b_0 \cdot p_0(x) + b_1 \cdot p_1(x) + \cdots + b_m \cdot p_m(x) = \sum_{k=0}^{m} b_k \cdot p_k(x)$.

- Comprueba que $p(a_i) = b_i$, para $i = 0, 1, \cdots, m$.

Ejercicio 21. Calcula las soluciones a los ejercicios 14 y 15 haciendo uso del método de Lagrange.

Ejercicio 22. Sea $A = \mathbb{Z}_2[x]_{x^3+1}$.

1. Calcula las unidades de A, y da, en cada caso, su inverso. ¿Es la suma de dos unidades una unidad? ¿Y el producto?

2. Calcula los divisores de cero. Para cada uno de ellos, encuentra un elemento no nulo de A que al multiplicarlo por él de cero. ¿Es la suma de dos divisores de cero un divisor de cero? ¿Y el producto?.

Ejercicio 23. Sea $A = \mathbb{Z}_5[x]_{x^3+3}$, y $\alpha = [x] \in A$.

- Comprueba que $3\alpha^2 + 4\alpha + 1$ y $2\alpha + 3$ son unidades y calcula sus inversos.
- Comprueba que $3\alpha^2 + 3$ y $4\alpha^3 + \alpha^2 + 3\alpha + 1$ son divisores de cero. Multiplícalos por un elemento no nulo de A para que de cero.

Ejercicio 24. Sean $K_1 = \mathbb{Z}_2[x]_{x^4+x+1}$ y $K_2 = \mathbb{Z}_2[x]_{x^4+x^3+x^2+x+1}$. Sean $\alpha = [x]$ y $\beta = [x]$, tomadas respectivamente en K_1 y K_2.

Calcula todas las potencias de α y β, y encuentra un isomorfismo $K_2 \to K_1$.